IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Vincent Dupaquis et al. PATENT APPLICATION
Serial No.: 10/781,311 Group Art Unit: 2131
Filed: February 18, 2004 Examiner:
For: RANDOMIZED MODULAR REDUCTION METHOD AND HARDWARE THEREFOR

Supplemental Information Disclosure Statement

Hon. Commissioner for Patents
Alexandria, VA 22313

Sir:

The following information is submitted in compliance with Applicants' duty of disclosure under 37 CFR § 1.56. A copy of each reference is enclosed.

Other References

A. Bosselaers et al., "Comparison of Three Modular Reduction Functions", Advances in Cryptology/Crypto '93, LNCS 772, Springer-Verlag, 1994, pp. 175-186.

C.H. Lim et al., "Fast Modular Reduction With Precomputation", preprint, 1999 (available from CiteSeer Scientific Literature Digital Library, 15 pages.

Jean Francois Dhem, "Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards", doctoral dissertation, Université catholique de Louvain, Louvain-la-Neuve, Belgium, May 1998.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Asst. Commissioner for Patents, Alexandria, VA 22313

Signed: Sally Azevedo
Typed Name: Sally Azevedo

Date: May 24, 2004

Respectfully submitted,

Thomas Schneck

Thomas Schneck
Reg. No. 24,518
P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733

ATM39:244.IDS

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicant: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Grant Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Grant Date	Country	Class	Sub Class	Translation Yes	Translation No
	AJ							
	AK							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AL	A. Bosselaers et al., "Comparison of Three Modular Reduction Functions", Advances in Cryptology/Crypto '93, LNCS 772, Springer-Verlag, 1994, pp. 175-186.
	AM	C.H. Lim et al., "Fast Modular Reduction With Precomputation", preprint, 1999 (available from CiteSeer Scientific Literature Digital Library, 15 pages.
	AN	J.F. Dhem, "Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards", doctoral dissertation, Université catholique de Louvain, Louvain-la-Neuve, Belgium, May 1998.

EXAMINER:	DATE CONSIDERED:

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.